Patent Claims

1. A method for protected execution of a cryptographic calculation, in which a key (12) with at least two key parameters (p, q, pinv, sp, dp, sq, dq) is drawn on, characterized in that an integrity check (30, 34, 40, 54) of the key (12) is performed, in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter (p, q, pinv, sp, dp, sq, dq) by corrupting at least one first key parameter (p, q, pinv, sp, dp, sq, dq).

2. A method as claimed in claim 1, characterized in that in the integrity check (30, 34, 40, 54) it is determined whether the value of at least one key parameter (p, q, pinv, sp, dp, sq, dq) is contained in a range of valid values, wherein the range is non-contiguous in that it has a plurality of gaps.

3. A method as claimed in claim 1 or claim 2, characterized in that in the integrity check (30, 34, 40, 54) it is determined whether at least two key parameters (p, q, pinv, sp, dp, sq, dq) are in a predetermined relationship to one another.

4. A method as claimed in one of claims 1 to 3, characterized in that the integrity check (30, 34, 40, 54) includes a multiplicative operation, in particular a divisibility test.

5. A method as claimed in one of claims 1 to 4, characterized in that in the integrity check (30, 34, 40, 54) it is checked whether a key parameter (p, q, pinv, sp, dp, sq, dq) or a value which differs from the key parameter (p, q, pinv, sp, dp, sq, dq) by a multiple of a safeguard value (sp, sq) is evenly divisible by the safeguard value (sp, sq).

6. A method as claimed in one of claims 1 to 5, characterized in that in the integrity check a checksum stored with the key parameters (p, q, pinv, sp, dp,

sq, dq) is compared with a checksum newly calculated after passing of the key parameters (p, q, pinv, sp, dp, sq, dq).

7. A method as claimed in one of claims 1 to 6, characterized in that, to check the integrity, important parameters to be passed are multiply passed and checked for identity after passing.

8. A method as claimed in one of claims 1 to 7, characterized in that the cryptographic calculation is a decryption or signature generation in an RSA method, in particular an RSA-CRT method.

9. A method as claimed in claim 8, characterized in that in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check (30, 34, 40, 54) it is checked whether the exponent used in the exponentiation operation is evenly divisible by a safeguard value (sp, sq).

10. A method as claimed in claim 9, characterized in that in the cryptographic calculation an exponent blinding method is applied for protection against spying.

11. A method as claimed in one of claims 8 to 10, characterized in that the prime factors (p, q) of the RSA method are multiplied by a masking parameter (j) and the error freedom of the calculation sequence is checked by an equality check modulo the masking parameter (j).

12. A method for determining a key for a cryptographic calculation with at least two key parameters (p, q, pinv, sp, dp, sq, dq), provided for use in a method as claimed in one of claims 1 to 9.

13. A method as claimed in claim 12, characterized in that at least one key parameter (p, q, pinv, sp, dp, sq, dq), is obtained by multiplication of a value required for the cryptographic calculation by a safeguard value (sp, sq).

14. A computer program product which has program commands to cause a processor to execute a method with the features of one of claims 1 to 13.

15. A portable data carrier, in particular a smart card or chip module, set up for executing a method with the features of one of claims 1 to 13.